**CHAROTAR UNIVERSITY OF SCIENCE AND TECHNOLOGY**
**Chandubhai S. Patel Institute of Technology**
**CHARUSAT Campus, Highway 139,**
**Off, Nadiad - Petlad Road,**
**Changa, Gujarat 388421**

**B.TEC. CSE SEM-III** **YEAR 2023**

**SUBJECT & SUBJECT CODE: DISCRETE MATHEMATICS & ALGEBRA (MA253)**

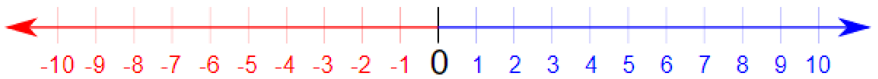
## CHAPTER: ABSTRACT ALGEBRA

**TOPICS INCLUDED ARE**

- **BASIC CONCEPT**
- **BINARY OPERATIONS**
- **COMPOSITION TABLE/ COMPOSITE TABLE.**
- **ALEGBRAIC STRUCTURE**
- **GROUPOID.**
- **SEMI GROUP**
- **MONOID**
- **GROUP AND ABELIAN GROUP.**
- **ORDER OF THE GROUP AND ELEMENT**
- **SUBGROUP**
- **LAGRANGE' S THEOREM**
- **CYCLIC GROUP**
- **PERMUTATION GROUP**

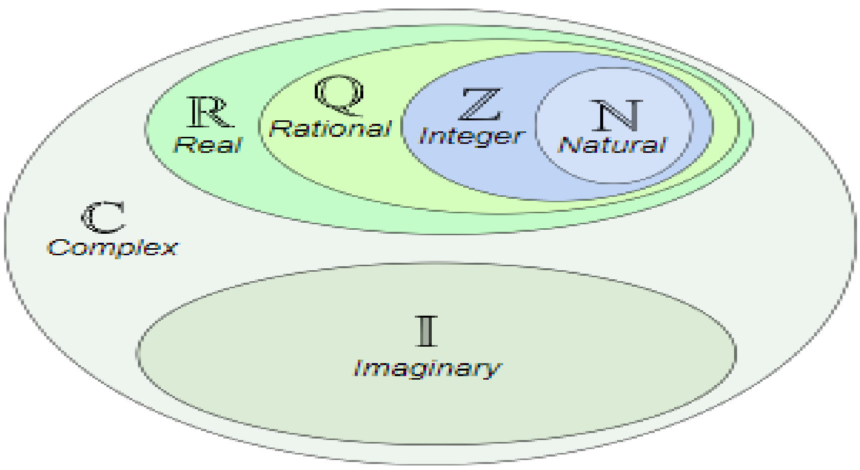
## BASIC CONCEPT

**COMMON NUMBER SETS:** There are sets of numbers that are used so often they have special names and symbols:

| Symbol | Descriptions |
|---|---|
| $\mathbb{N}$ | Set of Natural Numbers. |
| | Also known as Counting Numbers. |
| | The set is $\mathbb{N} = \{1, 2, 3, 4, 5, 6, ...............\}$ |
| $W$ | Set of Whole Numbers. |
| | $W = \{0, 1, 2, 3, 4, 5, ......\}$ |
| | $\mathbb{N} \subset W$ |
| $\mathbb{Z} / I$ | The whole numbers, {1,2,3,...} negative whole numbers {..., -3,-2,-1} and zero {0}. So the set is {..., -3, -2, -1, 0, 1, 2, 3, ...} |
| |  |

| | |
|---|---|
| | $\mathbb{Z}/I=\{..................-4,-3,-2,-1,0,1,2,3,4,5,......\}$ |
| | $\mathbb{N}\subset W\subset\mathbb{Z}$ |
| $\mathbb{Q}$ | Set of Rational Numbers. |
| | $\mathbb{Q}=\left\{\frac{p}{q}: p\ and\ q\ are\ \mathrm{int}\,egres\ and\ q\neq 0\right\}$ |
| | Property of rational number: Decimal expansion is terminating or recurring |
| | $\mathbb{N}\subset W\subset\mathbb{Z}\subset\mathbb{Q}$ |
| **Irrational Number** | No standard Notation |
| | Number which are not rational numbers. |
| | Property of irrational number: Decimal expansion is non-terminating or non-recurring. |
| $\mathbb{R}$ | Set of real numbers. |
| | All Rational and Irrational numbers. They can also be positive, negative or zero. |
| | $\mathbb{N}\subset W\subset\mathbb{Z}\subset\mathbb{Q}\subset\mathbb{R}$ |
| $\mathbb{C}$ | Set of Complex Number. |
| | Set of real numbers and the numbers of the form *a+ib*. |
| | $\mathbb{N}\subset W\subset\mathbb{Z}\subset\mathbb{Q}\subset\mathbb{R}\subset\mathbb{C}$ |

From the figure, it is clear that $\mathbb{N}\subset W\subset\mathbb{Z}\subset\mathbb{Q}\subset\mathbb{R}\subset\mathbb{C}$.




**BINARY OPERATION/BINARY COMPOSITION:** A binary composition or binary operation on a non empty set A is a mapping $f: A\times A\to A$.Suppose $a,b\in A$,then the image of (a,b) under a binary composition/operation o defined by aob.

**COMPOSITION TABLE** : A binary composition ( operation) on the non empty finite set A can be defined by table is called a composition table.

**Example: The composition table for multiplication modulo 7 on the set G={1,2,3,4,5,6}**

| $\times_7$ | **1** | | **2** | **3** | **4** | **5** | **6** |
|---|---|---|---|---|---|---|---|
| **1** | 1 | | 2 | 3 | 4 | 5 | 6 |
| **2** | 2 | | 4 | 6 | 1 | 3 | 5 |
| **3** | 3 | | 6 | 2 | 5 | 1 | 4 |
| **4** | 4 | | 1 | 5 | 2 | 6 | 3 |
| **5** | 5 | | 3 | 1 | 6 | 4 | 2 |
| **6** | 6 | | 5 | 4 | 3 | 2 | 1 |

**ALEGBRAIC STRUCTURE**: A non empty set G with one or more binary operations is called an algebraic structure.Suppose * is a binary operation on G.Then (G,*) is an algebraic structure.( N,+), (Z,+),(Z,-) are all algebraic structure.

**GROUPOID:** Suppose G is non empty set and o is a binary composition/operation then (G,o) is called a groupoid if o is closed in G, that is , given any two elements $a,b \in G \Rightarrow aob \in G$

**SEMI GROUP:** A non empty set G together with binary operation o,(G,o) is a semi group if binary opaeration o is commutative.

**IDENTITY ELEMENT:** There exist an element $\boldsymbol{e}$ G such that

$$\boldsymbol{a * e = a = e * a}, \forall \boldsymbol{a \epsilon G}$$

The element e is called the identity.

**MONOID:** A non empty set G together with a binary operation o,(G,o) is called a monoid if it satisfies the following properties:

1. o is closed in (G,o).
2. o is associative in (G,o)
3. There exist an identity element in (G,o)

**Example: The set of all integers Z with operation defined by a*b=a+b+1.**

1. **Is Z Groupoid?**
2. **Is Z a Semi Group?**
3. **Is Z a monoid?**

**Solution:**

**Groupoid: To prove G is groupoid ,prove that G is closed w.r.t ***

**Let** $a,b \in Z \Rightarrow a+b+1 \in Z$ ( Sum of integers is always an integer)

$a*b \in G$

Therefore G is closed w.r.t to operation*.

G is a groupoid.

**Semi Group: To prove G is Semigroup ,prove that * is associative i.e., to prove (a*b)*c=a*(b*c).**

**Let** $a,b,c\in Z$

L.H.S: $(a*b)*c=(a+b+1)*c=a+b+1+c+1=a+b+c+2$

R.H.S: $a*(b*c)=a*(b+c+1)=a+b+c+1+2=a+b+c+2$

L.H.S= R.H.S

Therefore * is associative.

**Monoid: To prove G is monoid, G must satisifes closure property, Associative property, identity property.**

**Closure property: Let** $a,b\in Z\Rightarrow a+b+1\in Z$ ( Sum of integers is always an integer)

$a*b\in G$

Therefore G is closed w.r.t to operation*.

**Associative property: Let** $a,b,c\in Z$

L.H.S: $(a*b)*c=(a+b+1)*c=a+b+1+c+1=a+b+c+2$

R.H.S: $a*(b*c)=a*(b+c+1)=a+b+c+1+2=a+b+c+2$

**L.H.S= R.H.S**

Therefore * is associative.

**Existence of Identity:** Let $e\in G$ be the identity element of G.

$a*e=a=e*a\ \forall a\in G$

Now

| | |
|---|---|
| $a*e=a$ | $e*a=a$ |
| $a+e+1=a$ | $e+a+1=a$ |
| $e=-1\in G$ | $e=-1\in G$ |

Therfore -1 is the identity element.

**G is a monoid**

**GROUP**

**GROUP:**Let G be a non-empty set with a binary operator denoted by * .Then this algebraic structure (G,*) is a group, if the binary * satisfies the following properties:

1. **Closure property:** $\boldsymbol{a*b\epsilon G\quad \forall a,b\epsilon G}$
2. **Associativity:**$\boldsymbol{(a*b)*c=a*(b*c)\ \forall a,b\epsilon G}$
3. **Existence of Identity:** There exist an element e G such that

   $$\boldsymbol{a*e=a=e*a,\forall a\epsilon G}$$

   The element e is called the identity.
4. **Existence of Inverse:** Each element of G possesses inverse i.e.,

   $$\boldsymbol{a*b=e=b*a,\forall a\ \epsilon G}$$

**ABELIAN GROUP:** A group is said to be abelian or commutative if in addition to the above four properties the following properties is also satisfied i.e.

$$\boldsymbol{a*b=b*a,\forall a,b\ \epsilon G}$$

**Commutative:**

**FINITE GROUP & INFINITE GROUP:** If in a group G the underlying set G consists of a finite number of distinct elements then the group is called a finite group otherwise an infinite group.

**EXAMPLE OF GROUP**

**Example: Show that the set I of all integers**

**…………………………..-4,-3,-2,-1,0,1,2,3,4,…………………………**

**is a group with respect to the operation of addition of integers.**

**Solution: Closure property:** We know that the sum of two integers is also an integer. i.e., a+b I .Thus I is closed w.r.t to addition.

**Associativity:** We know that addition of integers is an associative .Therefore a+(b+c)=(a+b)+c$\forall a, b , c \epsilon I$

**Existence of Identity:** The number $0\epsilon I$. Also we have

0+a=a=a+0.

Therefore 0 is the identity element.

**Existence of Inverse:**If$a \epsilon I$, then $-a \epsilon I$.Also we have

**a+ (-a)=0=(-a)+a.**

Thus every integer possesses additive inverse.

Therefore I is group with respect to addition .Since addition of integer is a commutative operator.

**Example:Show that the set of all positive rational number forms an abelian group under the composition defined by**

$$\boldsymbol{a * b = \frac{ab}{2}}$$

**Solution:** Let $Q_+$ denote the set of all positive rational number. To show: ($Q_+$, *) is a group.

**Closure Property:**

We know that multiplication and division of two rational number is a rational number therefore $\frac{\boldsymbol{ab}}{\mathbf{2}}$is a rational number. Thus for every a, b ∈ $Q_+$⇒ a*b∈ $Q_+$

Thus $Q_+$ is closed with respect to the operator *.

**Associativity:**Let a,b,c ∈ $Q_+$.Then

L.H.S: a*(b*c)=$a * \left(\frac{bc}{2}\right) = \frac{abc}{4}$

R.H.S: (a*b)*c=$\left(\frac{ab}{2}\right) * c = \frac{abc}{4}$

L.H.S=R.H.S

* is associative.

**Commutativity:** Let a,b∈ $Q_+$.Then

$$a * b = \frac{ab}{2} = \frac{ba}{2} = b * a$$

**Existence of Identity:** Let e be the identity element in $Q_+$.
By definition of identity element

$$a * e = a = e * a\ , \forall\ a \epsilon Q_+$$

**Now**

$$a * e = a \Longrightarrow \frac{ae}{2} = a \Longrightarrow \left(\frac{a}{2}\right)(e-2) = 0 \Longrightarrow e = 2\ since\ a\epsilon Q_+ \Longrightarrow a \neq 0$$
$$e * a = a \Longrightarrow \frac{ea}{2} = a \Longrightarrow \left(\frac{a}{2}\right)(e-2) = 0 \Longrightarrow e = 2\ since\ a\epsilon Q_+ \Longrightarrow a \neq 0$$

Therefore 2 is identity element.
**Existence if Inverse:** Let a be any element of $Q_+$.Let b be inverse of a then by definition of inverse

$$a * b = e = b * a$$

**Now** $\quad a * b = e \Longrightarrow \frac{ab}{2} = 2 \Longrightarrow b = \frac{4}{a}$

Now $a\epsilon Q_+ \Longrightarrow \frac{4}{a}\ \epsilon Q_+$

Now $\quad a * \frac{4}{a} = 2 = \frac{4}{a} * a$

Therefore $\frac{4}{a}$ is inverse of a .Thus each element of $Q_+$is inversible.
Hence ($Q_+$, *) is a group.

**Example: Show that the set$\boldsymbol{G = \left\{a + b\sqrt{2}:\ \ a, b, \in Q\right\}}$ is group with respect to addition.**
**Solution:**
**Closure Property:**Let x, y be any two elements of G. Then

$$\boldsymbol{x = a + b\sqrt{2}\,;\ y = c + d\sqrt{2}}$$

**Now**

$$\boldsymbol{x + y = a + b\sqrt{2} + c + d\sqrt{2}}$$
$$\boldsymbol{= (a + c) + (c + d)\sqrt{2}}$$

Since a+c and c+d are elements of Q, therefore$\boldsymbol{(a + c) + (c + d)\sqrt{2} \in G}$ **.**
Thus $x + y\epsilon G,\ \ \forall x, y\epsilon G$
Thus G is closed with respect to addition.
**Associativity:**The element of G are all real numbers and addition of real numbers is associative.

**Existence of Identity:** $0+0\sqrt{2} \in G$ since $0 \in Q$. If $a+b\sqrt{2}$ is any element of G, then

$$(a+b\sqrt{2})+0+0\sqrt{2}=a+b\sqrt{2}=0+0\sqrt{2}+(a+b\sqrt{2})$$

$0+0\sqrt{2}$ is the identity element.

**Existence of Inverse:** $\boldsymbol{a}+b\sqrt{2}\,\epsilon G \Rightarrow (-a)+(-b)\sqrt{2}\,\epsilon G$ since $a,b,\in Q \Rightarrow -a,-b,\in Q$

Now

$$(\boldsymbol{a}+\boldsymbol{b}\sqrt{\boldsymbol{2}})+\left((-\boldsymbol{a})+(-\boldsymbol{b})\sqrt{\boldsymbol{2}}\right)=\boldsymbol{0}+\boldsymbol{0}\sqrt{\boldsymbol{2}}$$

$$=(-\boldsymbol{a})+(-\boldsymbol{b})\sqrt{\boldsymbol{2}}+(\boldsymbol{a}+\boldsymbol{b}\sqrt{\boldsymbol{2}})$$

Therefore $(-\boldsymbol{a})+(-\boldsymbol{b})\sqrt{\boldsymbol{2}}$ is inverse element.

**Example: Show that the set of all matrices of the form $\begin{bmatrix} x & x \\ x & x \end{bmatrix}$,where x is a non zero real number, is a group of singular martices for multiplication.Find the identity and inverse of an element.**

**Solution:**Let $M=\left\{\begin{bmatrix} x & x \\ x & x \end{bmatrix} : x \text{ is a non}-\text{zero real number}\right\}$

**Closure Property**: Let $A=\begin{bmatrix} x & x \\ x & x \end{bmatrix} \in M,\ B=\begin{bmatrix} y & y \\ y & y \end{bmatrix} \in M$ where x and y are non zero real number.

Now $AB=\begin{bmatrix} x & x \\ x & x \end{bmatrix}\begin{bmatrix} y & y \\ y & y \end{bmatrix}=\begin{bmatrix} 2xy & 2xy \\ 2xy & 2xy \end{bmatrix} \in M$ because 2xy is also a non zero real number.

**Associativity:** Matrix Multiplication is always associative.

**Existence of identity:** Let $E=\begin{bmatrix} e & e \\ e & e \end{bmatrix} \in M$ such that $E.A=A\ \forall A \in M$ .Let $A=\begin{bmatrix} x & x \\ x & x \end{bmatrix} \in M$, .Then

$$EA=A \Rightarrow \begin{bmatrix} e & e \\ e & e \end{bmatrix}\begin{bmatrix} x & x \\ x & x \end{bmatrix}=\begin{bmatrix} x & x \\ x & x \end{bmatrix} \Rightarrow \begin{bmatrix} 2ex & 2ex \\ 2ex & 2ex \end{bmatrix}=\begin{bmatrix} x & x \\ x & x \end{bmatrix} \Rightarrow 2ex=x \Rightarrow e=\frac{1}{2} \operatorname{since} x \neq 0$$

Thus $E=\begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} \in M$ and is such that $E.A=A=A.E \quad \forall A \in M$

**Existence of inverse:** Let $C=\begin{bmatrix} c & c \\ c & c \end{bmatrix}\in M$ such that $\mathrm{C}.A=E \ \ \forall A\in M$ .Let $A=\begin{bmatrix} x & x \\ x & x \end{bmatrix}\in M$,

.Then

$$CA=A\Rightarrow\begin{bmatrix} c & c \\ c & c \end{bmatrix}\begin{bmatrix} x & x \\ x & x \end{bmatrix}=\begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}\Rightarrow\begin{bmatrix} 2cx & 2cx \\ 2cx & 2cx \end{bmatrix}=\begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}\Rightarrow 2cx=\frac{1}{2}\Rightarrow c=\frac{1}{4x}$$

Thus $C=\begin{bmatrix} \frac{1}{4x} & \frac{1}{4x} \\ \frac{1}{4x} & \frac{1}{4x} \end{bmatrix}\in M$ and is such that $\mathrm{C}.A=E=A.\mathrm{C} \ \ \forall A\in M$

Thus $C=\begin{bmatrix} \frac{1}{4x} & \frac{1}{4x} \\ \frac{1}{4x} & \frac{1}{4x} \end{bmatrix}\in M$ is inverse of A.

Hence M is a group w.r.t martix multiplication.

**Example : Prove that the set S of all ordered pairs (a,b) of real numbers for which** $a\neq 0$ **with respect to the operation X defined by ( a,b) X(c,d) = (ac, bc+d) is a group w.r.t X.**

**Solution: Closure Property:** Let (a,b) and (c,d) be any two element of S.Then $a\neq 0$ and $c\neq 0$.

Now ( a,b) X(c,d) = (ac, bc+d)$\in S$ ( because $a\neq 0$ and $c\neq 0\Rightarrow ac\neq 0$ )

Hence S is closed with respect to the given composition( binary operation)

**Associativity:** Let (a,b) , (c,d), (e,f) be any three element of S.

L.H.S $\left[(a,b)\times(c,d)\right]\times(e,f)$

$=(ac,bc+d)\times(e,f)$

$=\left(ace,(bc+d)e+f\right)=(ace,bce+de+f)$

**R.H.S**

$(a,b)\times\left[(c,d)\times(e,f)\right]$

$=(a,b)\times\left[(ce,\mathrm{de+f})\right]$

$=\left(ace,\mathrm{b}(ce)+de+f\right)=(ace,bce+de+f)$

**L.H.S=R.H.S**

Hence the given composition X is associative.

**Existence of Identity:** Let (x,y) be ientity element of S such that $(x,y)\times(a,b)=(a,b)=(a,b)\times(x,y)\Rightarrow(xa,ya+b)=(a,b)\Rightarrow xa=a;\ ya+b=b\Rightarrow x=1;\ y=0$

Therfore (1,0) is the identity element.

**Existence of Inverse:** Let (c,d) $\in S$ , $c \neq 0$ be inverse of (a,b) $\in S$ .

**Now** $(a,b)\times(c,d)=(1,0)=(c,d)\times(a,b)$

$\Rightarrow (ac, bc+d)=(1,0)$

$\Rightarrow ac=1;\ bc+d=0 \Rightarrow c=\frac{1}{a}\neq 0;\ d=-\frac{b}{a}$

$\left(\frac{1}{a},-\frac{b}{a}\right)$ is inverse of element (a,b).

**PRATICE EXAMPLE**

1.Do the following sets form groups with respect to binary operation * defined on them as follows:

- **a.** the set I of all integers with operation defined by a*b =a+b+1.
- **b.** the set Q of all rational number other than 1 , with the operation defined by a*b=a+b-ab.
- **c.** the set Q of all rational number other number than -1 with the operation defined by a*b=a+b+ab

2.Show that the set of all matrices $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$, and b being non-zero real numbers is a group under matrix multiplication .

3.If $G=\left\{\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} : a \text{ is any non} - \text{zero real number}\right\}$ .Show that G is a commutative group under matrix multiplication.

4.Show that the fourth roots of unity i.e., {1,-1,i,-i} form a group with respect to multiplication.

5. Show that the set G=$\{1,\omega,\omega^2\}$, where $\omega$ is an imaginary cube root of unity is a group with respect to multiplication.

6.Which is the identity element in the group G={ 2,4,6,8} under multiplication modulo 10?

7.Show that the set Z ,of all integers is a group under the binary operation * defined by a*b=a+b+2 for $\forall a,b \in Z$ .

8.Show that the set $\mathbb{Q}^+$, of all positive rational numbers forms commutative group under the binary operation * defined by $a * b = \frac{ab}{4}$., a, b $\in \mathbb{Q}^+$

## ORDER OF GROUP AND ORDER OF ELEMENT

**Order of a group:** The order of the group is defined as the number of element in the group.

**Order of an element:** Let G be a group with binary opaeration * .By the order of an element $a \in G$ is meant the least positive integer n,if one exists , such that $a^n$=e(the identity of G) .It is denoted by o(a).

**Remarks:** If there exists no positive integer n such that $a^n=e$, then we say that a is of infinite order or of zero order.

**Example : Find the order of each element of the multiplicative group { 1,-1,i,-i}.**

**Solution:** Since 1 is the identity element therefore o(1)=1.

| | |
|---|---|
| -1 | $(-1)^1=-1$ |
| | $(-1)^2= 1$ (i.e., identitiy element) $\therefore o(-1)=2$ |
| i | $(i)^1=i$ |
| | $(i)^2= -1$ (i.e., identitiy element) |
| | $(i)^3=-i$ |
| | $(i)^4= 1$ (i.e., identitiy element) $\therefore o(i)=4$ |
| -i | $(-i)^1=-i$ |
| | $(-i)^2= -1$ (i.e., identitiy element) |
| | $(-i)^3=i$ |
| | $(i)^4= 1$ (i.e., identitiy element) $\therefore o(-i)=4$ |

**Example : Find the order of each element of the group { 0,1,2,3,4,5} ,the composition being addition modulo 6.**

**Solution:** Since 0 is the identity element therefore o(0)=1.

| | |
|---|---|
| 1 | $(1)^1=1$ |
| | $(1)^2= 1+_61=2$ |
| | $(1)^3= 1+_61+_61=3$ |
| | $(1)^4= 1+_61+_61+_61=4$ |
| | $(1)^5= 1+_61+_61+_61+_61=5$ |
| | $(1)^6= 1+_61+_61+_61+_61+_61=0$(i.e., identitiy element) $\therefore o(i)=6$ |
| 2 | $(2)^1=2$ |
| | $(2)^2=2+_62= 4$ |
| | $(2)^3=2+_62+_62$ =2 0(i.e., identitiy element) $\therefore o(2)=3$ |
| 3 | $(3)^1=3$ |
| | $(3)^2= 3+_63=0$ (i.e., identitiy element) $\therefore o(3)=2$ |
| 4 | $(4)^1=4$ |
| | $(4)^2=4+_64= 8$ |
| | $(4)^3=4+_64+_64=$ 0(i.e., identitiy element) $\therefore o(4)=3$ |
| | $(5)^1=1$ |

| | |
|---|---|
| 5 | $(5)^2 = 5 +_6 5 = 4$ |
| | $(5)^3 = 5 +_6 5 +_6 5 = 3$ |
| | $(5)^4 = 5 +_6 5 +_6 5 +_6 5 = 2$ |
| | $(5)^2 = 5 +_6 5 +_6 5 +_6 5 +_6 5 = 1$ |
| | $(5)^2 = 5 +_6 5 +_6 5 +_6 5 +_6 5 +_6 5 = 0$(i.e., identitiy element) $\therefore o(5) = 6$ |

**Example: In the infinite multiplicative group of non zero rational numbers.Find the order of each element.**

**Solution:** Since " 1" is the identity element therefore o(1)=1.

$(-1)^1 = -1$; $(-1)^2 = 1$(identity element) therefore 0(-1)=2

Now $(2)^1 = 2$; $(2)^2 = 4$; $(2)^3 = 8$; $(2)^4 = 16$ and so on.Thus there exists no positive integer n such that $2^n = 1$(identity element). Therefore 0(2)= infinite.Similarly order of the remaining element is infinite.

**Example : Find the order of each element in the additive group of integers.**

**Solution:** Since " 0" is the identity element therefore o(0)=1.

Now $(1)^1 = 1$; $(1)^2 = 1+1 = 2$; $(1)^3 = 1+1+1 = 3$; $(1)^4 = 1+1+1+1 = 4$ and so on.Thus there exists no positive integer n such that $1^n = 0$(identity element). Therefore 0(1)= infinite.Similarly order of the remaining element is infinite.

**Remarks:**

1.The order of every element of a finite group is finite and is less than or equal to the order of the group.

2.The order of an element of a group is same as that of its inverse $a^{-1}$.

3.In an infinite group lement may be of finite as well as of infinite order.

**PRATICE EXAMPLE**

1. Consider the group G={ 1,2,4,7,8,11,13,14} under multiplication modulo 15.Find the order of the group and and order of the element 8 .

## SUBGROUP

**SUBGROUP:** A non empty subset H eof group is said to be subgroup of G if the binary operation in G is also a binary operation in H and for this operation H itself H itself is a group.

**Example :**

1.The multiplicative group { 1,-1} is a subgroup of the multiplicative group { 1,-1,I,-i}.

2.The additive group of even integer is a subgroup of the additive group of all integers.

3.The multiplicative group of positive rational numbers is a subgroup of the multiplicative of all non zero rational number.

**Remark:**

1.Every set is a subset of itself.Therefore if G is a group, then G itself is a group of G.Also if e is the identity of G,then the subset of G containing only one element i.e., e is also a subgroup of g.These two are subgroup of any group.They are called trivial or improper subgroup.A subgroup other than these two is called proper subgroup.

2.The identity of a subgroup is same as that of the group.

3.The inverse of any element of a subgroup is same as the inverse of the same regareded as an element of the group.

4.The order of any element of subgroup is the same as the order of the element regarded as a member of the group.

## CRITERION FOR A NON EMPTY SET TO BE A SUBGROUP

**Theorem 1:** A non empty subset H of a group G is a subgroup of G if and only if

(i). $a \in H, b \in H \Rightarrow ab \in H$

(ii). $a \in H \Rightarrow a^{-1} \in H$

**Theorem 2:** A necessary and sufficient condition for a non empty subset H of a group to be a subgroup is that $a \in H, b \in H \Rightarrow ab^{-1} \in H$ $b^{-1}$ is inverse of b in G.

## INTERSECTION OF SUBGROUP

**Theorem**: If $H_1$ and $H_2$ are two subgroup of a group G ,then $H_1 \cap H_2$ is also a subgroup of G.

**Proof**: Let $H_1$ and $H_2$ be any subgroup of G.Then $H_1 \cap H_2 \neq \phi$, since at lest the identity e is common to both $H_1$ and $H_2$.

In order to prove that $H_1 \cap H_2$ is a subgroup of G it is sufficient to prove that

$$a \in H_1 \cap H_2;\ b \in H_1 \cap H_2 \Rightarrow ab^{-1} \in H_1 \cap H_2$$

Now $a \in H_1 \cap H_2 \Rightarrow a \in H_1 \ and\ a \in H_2$

$b \in H_1 \cap H_2 \Rightarrow b \in H_1 \ and\ b \in H_2$

But $H_1$ and $H_2$ are subgroups.Therefore

$a \in H_1;\ b \in H_1 \Rightarrow ab^{-1} \in H_1$

$a \in H_2;\ b \in H_2 \Rightarrow ab^{-1} \in H_2$

Finally $ab^{-1} \in H_1$ and $ab^{-1} \in H_2 \Rightarrow ab^{-1} \in H_1 \cap H_2$.

Thus $a \in H_1 \cap H_2;\ b \in H_1 \cap H_2 \Rightarrow ab^{-1} \in H_1 \cap H_2$.

Hence $H_1 \cap H_2$ is a subgroup of G.

**Remark:** The union of two subgroup is not necessarily a subgroup.

**For example**, Let G be the additive group of integers.

Then $H_1$={………………….-6,-4,-2,0,2,4,6,…………}

$H_2$={………………….-12,-9,-6,-3,0,3,6,9,12…….} are two subgroup pf G.

$H_1 \cup H_2$={………………….-12,-10,-9,-6,-4,-3,-2,0,2,3,4,6,9,10,12……..}

Obviously $H_1 \cup H_2$ is not closed with respect to addition as $2 \in H_1 \cup H_2; 3 \in H_1 \cup H_2 \Rightarrow 5 \notin H_1 \cup H_2$

Therefore $H_1 \cup H_2$ is not a subgroup with respect to addition.

**Example: Let G be the additive group of integers.Then prove that the set of all multiples of integers by a fixed integer m is a subgroup of G.**

**Solution**: G={……………-3,-2,-1,0,1,2,3,………..} is the additive group of integer.

Let m be any fixed integer.

Let H={……………-3m,-2m,-1m,0,1m,2m,3m,………..}

Then $H \subseteq G$.

To prove that H is subgroup we prove $a \in H; b \in H \Rightarrow a-b \in H$.

Let a=rm and b=sm be any two element of H where r and s are some integer.Then inverse of sm in G is (-s)m i.e., -b=-sm.

Now a-b=rm+(-s)m=(r-s)m$\in H$ since r-s is also some intger.

Thus $a \in H; b \in H \Rightarrow a-b \in H$.

Therefore H is subgroup of G.

**Example: Let G be the set of all ordered pairs ( a,b) of real number for which** $a \neq 0$ **.Let a binary operation X on G be defined by the formula**

**(a,b) X(c,d)=(ac,bc+d)**

**Show that (G,X) is a non abelian group.**

**Does the subset H of all thoes elements of G which are of the form (1,b0 form a subgroup of G?**

**Solution: Closure Property:** Let (a,b) and (c,d) be any two element of S.Then $a \neq 0$ and $c \neq 0$.

Now ( a,b) X(c,d) = (ac, bc+d)$\in S$ ( because $a \neq 0$ and $c \neq 0 \Rightarrow ac \neq 0$ )

Hence S is closed with respect to the given composition( binary operation)

**Associativity:** Let (a,b) , (c,d), (e,f) be any three element of S.

L.H.S $\left[(a,b)\times(c,d)\right]\times(e,f)$

$=(ac,bc+d)\times(e,f)$

$=(ace,(bc+d)e+f)=(ace,bce+de+f)$

**R.H.S**

$(a,b)\times\left[(c,d)\times(e,f)\right]$

$=(a,b)\times\left[(ce,\text{de+f})\right]$

$=\left(ace,\mathrm{b}\left(ce\right)+de+f\right)=\left(ace,bce+de+f\right)$

L.H.S=R.H.S

Hence the given composition X is associative.

**Existence of Identity:** Let (x,y) be ientity element of S such that $\left(x,y\right)\times\left(a,b\right)=\left(a,b\right)=\left(a,b\right)\times\left(x,y\right)\Rightarrow\left(xa,ya+b\right)=(a,b)\Rightarrow xa=a;\ \ ya+b=b\Rightarrow x=1;\ y=0$

Therfore (1,0) is the identity element.

**Existence of Inverse:** Let (c,d) $\in S$ , $c\neq 0$ be inverse of (a,b) $\in S$ .

**Now** $\left(\mathrm{a,b}\right)\times\left(\mathrm{c,d}\right)=\left(1,0\right)=\left(\mathrm{c,d}\right)\times\left(\mathrm{a,b}\right)$

$\Rightarrow\left(\mathrm{ac,bc}+d\right)=(1,0)$

$\Rightarrow ac=1;\ \ bc+d=0\Rightarrow c=\dfrac{1}{a}\neq 0;\ d=-\dfrac{b}{a}$

$\left(\dfrac{1}{a},-\dfrac{b}{a}\right)$is inverse of element (a,b).

The inverse of (a,b) of G has been found to be $\left(\dfrac{1}{a},-\dfrac{b}{a}\right)$.

**To Prove H is a subgroup of G or not.**

Obviously H is a non empty subset of G.Let (1,b) and (1,c) be any two elements of H. Then

(1,b)X$(1,c)^{-1}$=(1,b)x$\left(\dfrac{1}{1},-\dfrac{c}{1}\right)$=(1,b-c) ( By definition of operation of G)

(1, b-c) is definitley an element of H.Thus

$(1,b),(1,c)\in H\Rightarrow(1,b)\times(1,c)^{-1}\in H$

Hence H is subgroup of G.

**Example:Let G be the multilicative group of all positive real numbers and R the additive group of all real numbers.Is G a subgroup of R?**

**Solution:** The set G of all positive real numbers is a subset of the set of R of all real numbers.But the group G is not a subgroup of the group R.The reason is that the composition/ binary operation in G is different from the composition/ binary operation in R.

**LAGRANGE'S THEOREM: The order of each subgroup of a finite group is a divisor of the order of the group.**

**Note:** Lagrange's therorem has every important applications.Suppose G is a finite group of order n.If m is not a divisor of n , then there can be no subgroup of order m.Thus if G is a group of order 6, then there can be no group of order 5 or 4.Similarly if G is a group of prime order p then G can have no proper subgroup.

# CYCLIC GROUP

**CYCLIC GROUP:** A group G is called cyclic for some $a \in G$ ,every element $x \in G$ is of the form $a^n$where n is some integer. The element **a** is then called a generator of G.

**Example:** The multiplicative group ={1,-1,i,-i} is cyclic .We can write G={ $i,i^2,i^3,i^4$}.Thus G is a cyclic group and I is a generator.Also we can write G={ $-i,(-i^2),(-i^3),(-i^4)$}.Thus –i is the generator of G.

**Example:** The multiplicative group $\{1,\omega,\omega^2\}$ is cyclic.The generators are $\omega,\omega^2$ .

**Example:** The group A=({0,1,2,3,4,5},$+_6$} is cyclic.This group is generated by 1 and another generator is 5.

**Remarks:**

1. Every cyclic group is an abelian.
2. If a is a generator of a cyclic group G,then $a^{-1}$ is also generator of G.
3. If "a" is a generator of an infinite cyclic group G, then the order of a must be infinite.If the order of a is finite ,then cyclic group generator by "a" is of finite order.Therefore the order of the cyclic group is equal to order of its generating element.
4. If a finite group of order n contains an element of order n, then group must be cyclic.
5. If the cyclic group G is generatted by an element a of order n, then $a^m$ is generator of G if and only if the greatest common divisor of m and n is 1 i.e., m and n is relatively prime.
6. If G is a cyclic group of order n then total number of generators of G will be equal to number of integer less than n and prime to n.For example if a is generator of a cyclic group G of order 8, then $a^3,a^5,a^7$ will be the only genertors of G.Since 4 is not prime to 8 therefore $a^4$ cannot be generator of G.Similarly $a^2,a^6,a^8$ cannot be generators of G.

**Example : Show that the group ({1,2,3,4,5,6},$x_7$) is cyclic .How many generators are there?**

**Solution:**Let G={1,2,3,4,5,6}. If there exists an element $a \in G$ such that 0(a)=6 i.e., the order of the group G then the group G will be cyclic group and a will be generator of G.

| | |
|---|---|
| 3 | $(3)^1=3$ |
| | $(3)^2= 3X_7 3=2$ |
| | $(3)^3= 3X_7 3X_7 3=3$ |
| | $(3)^4= 3X_7 3x_7 3x_7 3=4$ |
| | $(3)^5= 3X_7 3X_7 3X_7 3x_7 3=5$ |

| | |
|---|---|
| | $(3)^6 = 3X_7 3x_7 3X_7 3X_7 3X_7 3 = 1$(i.e., identitiy element) $\therefore o(3) = 6$ |

Since O(3)=6= order of the group therefore G is a cyclic group and 3 is a generator of G.

Now If a is a generator of a cyclic group G,then $a^{-1}$ is also generator of G.

Therefore 5 is also generator of the group.

**PRATICE EXAMPLE**

) Is the group G={ 1,3,5,7} cyclic w. r. t $\times_8$ ? Justify your answer.

## PERMUTATION GROUP

**Definition:** Suppose S is a finite set having n distinct elements.Then a one-one mapping of S onto itself is called a permutation of degree n.

The number of elements in the finite set S is known as the degree of permutation.

**Total number of distinct permutation of degree:n!**

**Equality of two permutation:** Two permutation f and g of degree n said to be equal if we have f(a)=g(a) $\forall a \in S$.

**Product or Composite of two Permutation:** The product or composite of two composite of two permutation f and g of degree n degree n denoted by fg , is obtained by first carrying out the operation defined by f and then by g.

Example: Let $f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ $g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ be two permutation of degree 3.Then

$$fg = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$gf = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Obviously $fg \neq gf$

**Example: Show the set $P_3$ of all permutaion on three symbols 1,2,3 is a finite non abelian group of order with respect to permutation multiplication as composition.**

**Solution:** $P_3$={ I, ( 1 2), (2 3) , (3 1), (1 2 3), (1 3 2)}

Let $f_1$=I, $f_2$= ( 1 2) , $f_3$=(2 3), $f_4$= (3 1) ,$f_4$ =(1 2 3), $f_5$ =(1 3 2)

| Product of Permutations | $f_1$ | $f_2$ | $f_3$ | $f_4$ | $f_5$ | $f_6$ |
|---|---|---|---|---|---|---|
| $f_1$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ | $f_5$ | $f_6$ |
| $f_2$ | $f_2$ | $f_1$ | $f_6$ | $f_5$ | $f_4$ | $f_3$ |
| $f_3$ | $f_3$ | $f_5$ | $f_1$ | $f_6$ | $f_2$ | $f_4$ |
| $f_4$ | $f_4$ | $f_6$ | $f_5$ | $f_1$ | $f_3$ | $f_2$ |
| $f_5$ | $f_5$ | $f_3$ | $f_4$ | $f_2$ | $f_6$ | $f_1$ |
| $f_6$ | $f_6$ | $f_4$ | $f_2$ | $f_3$ | $f_1$ | $f_5$ |

**Closure Property:** Since all the entries in the table are elemet of $P_3$, therefore $P_3$ is cosed with respect to multiplication of permutation.

**Associative Property:** Multiplication of permutation is always associative.

**Existence of Identity :** From the table , $f_1$ is the identity element.

**Existence of Inverse:**

$(f_1)^{-1}=f_1$; $(f_2)^{-1}=f_2$; $(f_3)^{-1}=f_3$; $(f_4)^{-1}=f_4$; $(f_5)^{-1}=f_6$; $(f_6)^{-1}=f_5$

Thus inverse of each element exist.

Since $P_3$ satisfies all the condition therefore $P_3$ is a group w.r.t permutation multiplication.